## Remarks

Applicants respectfully request reconsideration of the present U.S. Patent application as amended herein. Claims 10 and 24 have been amended. Claims 28-29 have been canceled. No claims have been added. Thus, claims 1-27 are pending.

CLAIM REJECTIONS – 35 U.S.C. § 112, SECOND PARAGRAPH

Claims 10 and 12 were rejected as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. Claim 10 has been amended to provide proper antecedent basis. Claim 12 was rejected as reciting "a network unit" however, claim 12 does not recite a network unit. Applicants assume that this rejection was the result of a typographical error.

CLAIM REJECTIONS – 35 U.S.C. § 103(a)

Claims 1-29 were rejected as being unpatentable over U.S. Patent No. 6,347,376 issued to Attwood, et al (*Attwood*) in view of U.S. Patent No. 6,253,321 issued to Nikander, et al. (*Nikander*). Claims 28 and 29 have been canceled. Therefore, the rejection of claims 28 and 29 is moot. For at least the reasons set forth below, Applicants submit that claims 1-27 are not rendered obvious by *Attwood* and *Nikander*.

As a preliminary matter, Applicants note that the purpose of *Attwood* is to reduce the number of searches that may be required for IPsec operations. See col. 3. In contrast, the specification for the claimed invention states:

> In methods and apparatus for preventing packet retransmissions according to the present invention, a network interceptor (i.e., network shim) is placed between the application and the TCP/IP stack. When an application on one unit desires to communicate with another application on another unit across a network, the application uses a socket. A socket

> is an abstraction that is used to represent one end point of a network communication. Since the network interceptor is between the application and TCP/IP stack, all requests for network communication must go through the network interceptor. The network interceptor can, therefore, monitor specific socket requests to make sure that IPsec security associations are in place before any packets are allowed to flow. ***Therefore, erroneous packet retransmissions are prevented.***

See page 7, second full paragraph (emphasis added).

Claim 1 recites:

> determining if there is an active security association that exists to protect network flow associated with the connection request;
> ***preventing the connection request from proceeding*** if no active security association exists to protect the network flow...

Thus, Applicants claim preventing a connection request from proceeding. Claim 20 is directed to a machine readable medium having instructions to perform operations that include preventing the connection of a request from proceeding.

In contrast, *Attwood* discloses searching a static rule set if rule binding information is not available. See col. 11, lines 46-65. *Attwood* discloses making a secure TCP connection using Ipsec. However, *Attwood* does not disclose preventing a connection under certain conditions. Therefore, *Attwood* cannot teach the limitation for which it is cited to teach. Applicants agree that *Attwood* does not disclose whether a security association is manual configured or dynamically negotiated. However, whether or not *Nikander* discloses this limitation, *Nikander* does not cure the deficiencies of *Attwood*. Therefore, because neither *Attwood* nor *Nikander* teach or suggest preventing a connection, no combination of *Attwood* and *Nikander* can teach or suggest the invention as claimed in claims 1 and 20.

Claims 2-9 depend from claim 1. Claims 21-23 depend from claim 20. Because dependent claims include the limitations of the claims from which they depend,

Applicants submit that claims 2-9 are not anticipated by *Attwood* and *Nikander* for at least the reasons set forth above.

Claim 10 recites:

> determining what security policy should be used when negotiating a security association for the network flow if there is no defined security association that may be used to protect the network flow;
> preventing the UDP data from being sent if there is no defined security association that may be used to protect the network flow;
> alerting a security association negotiation component to initiate negotiation for the security association if there is no defined security association that may be used to protect the network flow;
> establishing the security association; and
> allowing the UDP data to be sent in response to establishment of the security association.

Thus, Applicants claim preventing UDP data from being sent under certain conditions and allowing the UDP data to be sent in response to establishment of a security association. Claims 11-16 depend from claim 10. Claim 24 is directed to a machine readable medium having instructions to perform operations that include preventing UDP data from being sent under certain conditions and allowing the UDP data to be sent in response to establishment of a security association. Claims 25-27 depend from claim 24.

As discussed above, no combination of *Attwood* and *Nikander* teaches or suggests preventing data from being transmitted in the absence of a defined security association. Therefore, no combination of *Attwood* and *Nikander* can teach or suggest the invention of claims 10-16 and 24-27.

Claim 17 recites:

> wherein the network interceptor insures that a security association is in place before allowing network traffic to flow between the application and the network unit.

Thus, Applicants claim a network interceptor that insures a security association is in place before allowing network traffic to flow. Claims 18 and 19 depend from claim 17.

As discussed above, no combination of *Attwood* and *Nikander* teaches or suggests preventing data from being transmitted in the absence of a defined security association. Therefore, no combination of *Attwood* and *Nikander* can teach or suggest a network interceptor that insures a security association is in place before allowing network traffic to flow. Accordingly, no combination of *Attwood* and *Nikander* can teach or suggest the invention of claims 17-19.

CONCLUSION

For at least the foregoing reasons, Applicants submit that the rejections have been overcome. Therefore, claims 1-27 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application. Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
**BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP**

Date: July 26, 2004

Paul A. Mendonsa
Attorney for Applicant
Reg. No. 42,879

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(503) 439-8778